IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF:	
INFORMATION ASSOCIATED WITH INSTAGRAM ACCOUNT "MR.BLUE_30" STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	**CASE NO.** 8:24-mj-00505-TJS
INFORMATION ASSOCIATED WITH ANY INSTAGRAM ACCOUNTS ASSOCIATED WITH 240-722-9960 STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	**CASE NO.** 8:24-mj-00506-TJS
APPLE IPHONE ASSIGNED CALLING NUMBER 240-722-9960 CURRENTLY LOCATED AT DEA HIDTA, GREENBELT, MD 20770	**CASE NO.** 8:24-mj-00507-TJS
INFORMATION CONTAINED IN APPLE ICLOUD ACCOUNTS ASSOCIATED WITH 240-722-9960 STORED AT PREMISES CONTROLLED BY APPLE	**CASE NO.** 8:24-mj-00508-TJS

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Jacqueline Abadir, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Instagram accounts (**Target's Former Instagram Account** and **Additional Instagram Accounts**) which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachments A1 and A2. This affidavit is made in support of an application for a search warrant

under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B1 and B2. Upon receipt of the information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

2. I also submit this affidavit in support of an application under Federal Rule of Criminal Procedure Rule 41 for a search warrant authorizing the examination of property -an electronic device described herein and in Attachment A2 (the "**Target Device**") – that is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B3. This affidavit will show that there is probable cause to believe that the **Target Device** contain evidence of violations of 21 U.S.C. § 841 (possession with Intent to Distribute Controlled Substances) and 21 U.S.C. § 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances).

3. I additionally make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41, 18 U.S.C. §§ 2703(a), and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the phone number 240-722-9960 (the **Target's iCloud Account**), which was used by Franklin CARBAJAL GUERRA and is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A4 and Attachment B4.

4. I have been a DEA Special Agent since July 2017 and am currently assigned to the

Greenbelt High Intensity Drug Trafficking Area office out of the DEA Washington District Office. In this capacity, I investigate drug trafficking organizations operating throughout the Washington Metropolitan area. Prior to becoming a DEA Special Agent, I was a DEA Intelligence Analyst beginning in September 2008.

5. As a Special Agent, I am "an investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for the offenses enumerated in 18 U.S.C. § 2515.

6. As a DEA Special Agent and a DEA Intelligence Analyst, I have received extensive training in the enforcement of drug laws of the United States, as well as extensive training in criminal investigations. I also have participated in investigations involving unlawful narcotics distribution. As part of these investigations, I have been involved in the application for and execution of arrest and search warrants for narcotics related offenses, resulting in the prosecution and conviction of individuals and the seizure of illegal drugs, weapons, illegal drug proceeds, and other evidence of criminal activity. As a narcotics investigator, I have interviewed individuals involved in drug trafficking and have obtained information from them regarding the acquisition, sale, importation, manufacture, and distribution of controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology used by traffickers of controlled dangerous substances. Since 2008, I have supported and participated in narcotics investigations, which have led to the arrest and conviction of members belonging to drug trafficking organizations.

7. I have training and experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, surveillance, undercover operations, operations involving

cooperating sources, and a variety of other investigative tools available to law enforcement officers. During my training and experience, I have become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of proceeds derived from the sale of narcotics, and the organization of drug conspiracies. In the course of conducting these investigations, I have been involved in the use of the following investigative techniques, among others: interviewing sources of information and cooperating sources; conducting physical surveillance; conducting short-term and long-term undercover operations, including reverse undercover operations; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification data; conducting court-authorized electronic surveillance; and preparing and executing search warrants that have led to substantial seizures of narcotics, firearms, and other contraband.

8. As a result of this training and experience, I learned that individuals who traffic narcotics or firearms routinely use cellular telephones, personal data devices ("PDAs"), computers, external hard drives, thumb drives, CDs/DVDs, and other electronic media to facilitate their trafficking and money laundering operations. Further, individuals who engage in narcotics or firearms trafficking, do so in an ongoing process that requires the development and use of a secure communication network to facilitate daily contact with coconspirators and potential purchasers of narcotics and/or firearms or with customers and people involved in the laundering of funds. Oftentimes, this secure communications network is accomplished by text message, SMS, MMS, or Direct Message via various social media platforms, such as Facebook and Instagram. Narcotics and firearms traffickers use the above-described devices and platforms to maintain contact with their customers and/or accomplices and keep records and ledgers, including photos, GPS coordinates, and descriptions of potential narcotics or firearms that they are aiming to traffic.

9. Based on my training and experience, and the training and experience of other agents/officers with whom I am working on this investigation, I know that persons who engage in narcotics or firearms trafficking activities often use social media platforms to communicate with coconspirators and/or customers and send photographs of firearms. To attempt to secrete their activities, traffickers download social media applications on their cellular telephones, PDAs, or other digital devices that have the capability to communicate with one another using encryption applications that aide in defeating law enforcement detection.

10. I am familiar with the facts and circumstances of the investigation through discussions with other law enforcement agencies and from my review of records and reports relating to the investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

11. This affidavit is made in support of an application for a warrant to search the **Target's Former Instagram Account**, **Additional Instagram Accounts**, **Target Device**, and **Target's iCloud Account** for evidence in connection to a fatal overdose fentanyl[1] death.

12. This court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States (including a magistrate judge of such a court) . . . that . . . has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

[1] Fentanyl is a Schedule II controlled dangerous substance.

13. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C) have been committed by Franklin CARBAJAL GUERRA, alias "Mr.Blue_30" (the user name associated with **Target's Former Instagram Account**) and other persons known and unknown. I have reason to believe that additional records contained in the **Target's Former Instagram Account, Additional Instagram Accounts, Target Device,** and **Target's iCloud Account** contain evidence identifying and linking a victim, suspect, and possible witnesses to the crimes of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C). There is also probable cause to believe that the information described in Attachments A1, A2, A3, and A4 contain evidence of these crimes, as further described in Attachments B1, B2, B3 and B4.

PROBABLE CAUSE

14. On December 2, 2022, at approximately 7:01 am, a Prince George's Police Department (PGPD) officer responded to a 911 call for service at 4803 Glenoak Road, Hyattsville, MD 20784; "the victim's residence," to assist Prince George's County Fire and Rescue ("Fire/Rescue") personnel. Upon arrival, the PGPD officer was advised by Fire/Rescue that when they arrived at the victim's residence, they observed 15-year-old Yessina Morales Yaque was unconscious and not breathing. Fire/Rescue personnel conducted CPR. Yessina Morales Yaque was pronounced dead at 7:13 am. Her body was transported to the Office of the Chief Medical Examiner for an autopsy.

15. While at the victim's residence, PGPD officers spoke to Maria Morales Yaque, Yessina's mother, who stated that she last saw Yessina alive on December 1, 2022 at approximately 11:00 pm. Maria advised that when she woke up to go to work on December 2, 2022 at approximately 5:00 am, she did not notice Yessina in their bedroom and went to try to

use the bathroom.[2] At this time, Maria advised she waited approximately fifteen minutes and attempted to call Yessina with a negative response. Maria then opened the bathroom door and observed Yessina face down on the floor. At this time, Maria dragged Yessina into her bedroom, where she laid Yessina down on the bed. After approximately an hour later, Maria observed that Yessina was still unresponsive and called 911.

16. Fire/Rescue personnel located a quarter and a half of one (1) small, blue, round pill in a small glassine baggie located on the bathroom sink. The pill was submitted to the PG County Crime Laboratory for analysis. Additional PGPD officers responded to the victim's residence. PGPD officers located Yessina's iPhone, phone number 240-302-4896. Maria confirmed that the iPhone was in fact Yessina's. The iPhone was seized by PGPD officers. The contents of the iPhone were later extracted.

17. On December 3, 2022, Assistant Medical Examiner Dr. Avneesh Gupta performed an autopsy on Yessina's body. Dr. Gupta concluded Yessina's death was caused by fentanyl intoxication.

18. Investigators located an Instagram text message chain with Mr.Blue_30, **Target's Former Instagram Account**, on Yessina's iPhone. I know from my training and experience that fentanyl is commonly distributed in counterfeit oxycodone pills that appear light blue and have the number "30" stamped on them, so "mr.blue_30" was an explicit reference to being a dealer of such substances. On December 1, 2022, starting at approximately 7:58 pm, Yessina had the following conversation with the **Target Former Instagram Account**. [3]

[2] Maria Morales Yaque and Yessina shared a bedroom and a bathroom.

[3] There was no other time stamp during Yessina's Instagram conversation with the **Target's Instagram Account**.

Yessina: "hello how much a pop?"
Yessina: "oh okay"
Yessina: "are you in wheel?
Yessina: "yess"
Yessina: "I have 20"
Yessina: "6908 Buchanan St, Hyattsvilel, MD 20764"[4]
Yessina: "Oh okay bett"
Yessina: "oh okay"
Yessina: "Coming"
Yessina: "Is that you with th elights on?"
Yessina: "I'm in front of you"
Yessina: "Thanks you so much"

19. Mr.Blue_30's side of the conversation was missing on Yessina's Instagram Account, and had apparently been deleted by the counterparty.

20. On June 16, 2023, United Stated Magistrate Judge Timothy J. Sullivan signed an Instagram search warrant affidavit for **Target's Former Instagram Account** for the limited period of November 30 to December 3, 2022. That Instagram return showed that that the Target Instagram account was activated on February 14, 2021, and disabled on January 24, 2023. The Instagram return also showed that CARBAJAL used **Target's Former Instagram Account** to communicate apparent fentanyl sales to several customers other than Yessina Morales-Yaque during that four-day window, and was also missing his side of the conversation with Yessina on December 1, 2022.

21. The Instagram return information further revealed that phone number 240-643-0483 was associated to "mr.blue_30" and had provided the name of the user as "blues on the way" rather than a legal name. Law enforcement databases showed that Franklin CARBAJAL GUERRA was associated with the 240-643-0483 number during that time period. CashApp records between January 20, 2021, and July 16, 2023, also showed CARBAJAL GUERRA's account as being

[4] 6908 Buchanan Street, Hyattsville, MD is approximately three (3) houses away from the victim's residence.

associated to 240-643-0483 during this period. T-Mobile subscriber return data showed that 240-643-0483 was activated on September 28, 2020 and deactivated on March 3, 2023. Common call analysis conducted suggested that phone number 240-722-9960 (hereinafter the "**Target Device"**) was CARBAJAL GUERRA's replacement for 240-643-0483. AT&T subscriber return data listed that **Target Device** was activated on February 7, 2023 and subscribed to "Carlos Flores."

22. On January 25, 2024, following the return of an indictment charging him with distribution of fentanyl leading to Yessina Morales-Yaque's death, United States Magistrate Judge Gina L. Simms, District of Maryland, signed an arrest warrant for Franklin CARBAJAL GUERRA.

23. On February 7, 2024, Judge Peter Killough of the Circuit Court for Prince George's County signed a geo-location and cell site simulator warrant for the PGPD Fugitive Unit (FU) to track the **Target Device** in order to arrest CARBAJAL.

24. On February 8, 2024, your Affiant began receiving AT&T geo-locational data for the **Target Device.** The PGPD FU used the information provided by AT&T in conjunction with the cell site simulator to locate **Target Device** at 1403 Merrimac Drive, apartment 101, in Hyattsville, Maryland. The PGPD FU knocked at apartment 101; an older Hispanic male opened the door, at which point PGPD FU observed CARBAJAL GUERRA behind the older Hispanic male. CARBAJAL GUERRA was placed under arrest by the PGPD FU.

25. Once placed under arrest, TFO Fernando Jaramillo asked CARBAJAL GUERRA if he would like to make a phone call before officers escorted him to jail. CARBAJAL GUERRA indicated that he would and told officers that the phone he wanted to use was on the couch. TFO Jaramillo retrieved **Target Device**, a silver Apple iPhone, which CARBAJAL GUERRA unlocked for use.

BACKGROUND ON INSTAGRAM AND META

26. Instagram is a service owned by Meta Platforms, Inc., a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Facebook and Instagram accounts, like the **Target's Former Instagram Account** and **Additional Instagram Accounts** listed in Attachments A1 and A2, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

27. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Instagram keeps records of changes made to this information.

28. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

29. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

30. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Instagram maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

31. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

32. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

33. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on

privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

34. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

35. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

36. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

37. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

38. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

39. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

40. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

41. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

42. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Facebook maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

43. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

44. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

45. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

46. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and

experience, instant messages, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

47. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

48. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

49. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, the contact information for the Instagram account may reveal services used in furtherance of the crimes under investigation or services used to communicate with coconspirators.

50. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

TECHNICAL TERMS

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0–255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

52. Based on my training and experience, I know that the **Target Device** has capabilities that allow the device to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

53. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on cellular phones. This information can sometimes be recovered with forensics tools.

54. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target**

Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

55. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the cellular phones to human inspection in order to determine whether it is evidence described by the warrant.

Manner of execution. Because this warrant seeks only permission to examine cellular phones already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

BACKGROUND CONCERNING APPLE[5]

56. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

57. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

[5] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

58. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

59. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the

account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

60. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

61. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

62. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

63. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

64. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in

furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

65. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

66. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity,

documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

68. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

69. Based on the earlier search warrant returns of **Target's Former Instagram Account** showing evidence of fentanyl distribution, as well as CARBAJAL GUERRA's apparent deletion of his text messages with Yessina and disuse of the account altogether after her death, there is cause to believe the recorded communications it contains during the time period during which it was active (February 14, 2021, to January 24, 2023) will provide evidence both of CARBAJAL GUERRA's fentanyl distribution activities, but, more probative to the prosecution, evidence of his knowledge of, and responsibility for, Yessina Morales Yaque's death.

70. Based upon CARBAJAL GUERRA's apparent use of and control over the **Target Device**, along with his prior use of Instagram accounts associated with his prior phone number, there is cause to believe that the **Target Device** along with **Additional Instagram Accounts** and **Apple iCloud Account** associated with the **Target Device** beginning February 14, 2021, will provide evidence of continued violations of 21 U.S.C. § 841(a) that are relevant to his prosecution.

71. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Facebook and Apple. Because the warrant will be served on Meta and

Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Jacqueline Abadir
Special Agent
Drug Enforcement Administration

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 23rd day of February 2024.

Honorable Timothy J. Sullivan
United States Magistrate Judge

ATTACHMENT A1

Property to Be Searched

This warrant applies to information associated with Instagram account, **MR.BLUE_30**, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc., a company headquartered at 1601 Willow Road, Menlo Park, California.

ATTACHMENT B1

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 8, 2023, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from **February 14, 2021 to January 24, 2023**;

7. Privacy and account settings, including change history; and

8. Communications between Facebook and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from **February 14, 2021 to January 24, 2023**

C. All content, records, and other information relating to communications sent from or received by the Account from **February 14, 2021 to January 24, 2023** including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the Account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from **February 14, 2021 to January 24, 2023** including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account from **February 14, 2021 to January 24, 2023**; and

F. All location information, including location history, login activity, information geotags, and related metadata from **February 14, 2021 to January 24, 2023**.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes [[fruits, contraband, evidence, and instrumentalities]] of violations of 21 U.S.C. §§ 841(a) (1) and (b)(1)(C) and, those violations involving Instagram user ID **"MR.BLUE_30"** occurring from **February 14, 2021 to January 24, 2023** including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The stored communications and files (pictures, direct messages, and saved stories) associated with Instagram user ID "**MR.BLUE_30**"**.** Based on my training and experience the aforementioned communication techniques are used by drug traffickers to facilitate, purchase, and sale illegal drugs.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID "**MR.BLUE_30"** as it relates to the sale of controlled substances, specifically, from **February 14, 2021 to January 24, 2023**. Communication techniques (Instagram photographs, direct messages, and saved stories) under user ID "**MR.BLUE_30**" will help determine the level of communication between Franklin CARBAJAL GUERRA and unknown co-conspirators, including records that help reveal their whereabouts.

ATTACHMENT A2

Property to Be Searched

This warrant applies to information associated with any Instagram accounts associated with phone number 240-722-9960, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc., a company headquartered at 1601 Willow Road, Menlo Park, California.

ATTACHMENT B2

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A2 is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 8, 2023, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from **January 24, 2023 to February 8, 2024**;

7. Privacy and account settings, including change history; and

8. Communications between Facebook and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from **January 24, 2023 to February 8, 2024;**

C. All content, records, and other information relating to communications sent from or received by the Account from **January 24, 2023 to February 8, 2024** including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the Account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from **January 24, 2023 to February 8, 2024** including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account from **January 24, 2023 to February 8, 2024**; and

F. All location information, including location history, login activity, information geotags, and related metadata from **January 24, 2023 to February 8, 2024**.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes [[fruits, contraband, evidence, and instrumentalities]] of violations of 21 U.S.C. §§ 841(a) (1) and (b)(1)(C) and, those violations involving any Instagram accounts associated with phone number 240-722-9960 occurring from **February 14, 2021 to January 24, 2023** including, for each account or identifier listed on Attachment A2, information pertaining to the following matters:

(a) The stored communications and files (pictures, direct messages, and saved stories) associated with any Instagram accounts associated with phone number 240-722-9960**.** Based on my training and experience the aforementioned communication techniques are used by drug traffickers to facilitate, purchase, and sale illegal drugs.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

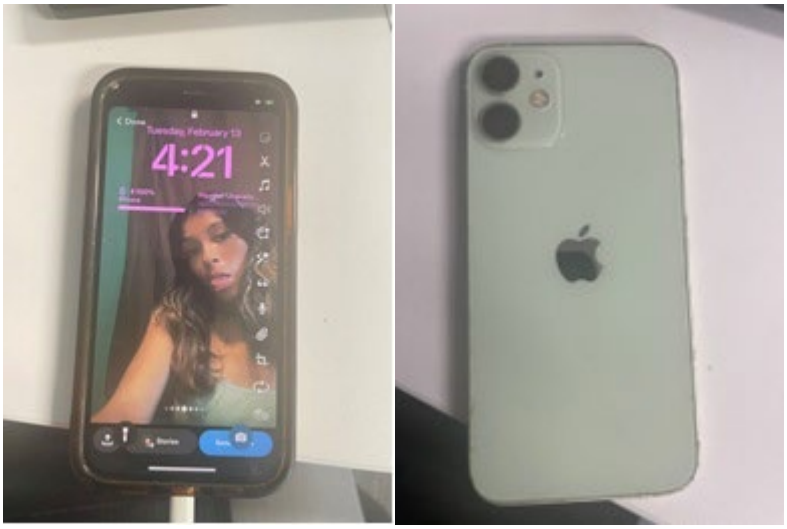
(e) The identity of the person(s) who communicated with any Instagram accounts associated with phone number 240-722-9960 as it relates to the sale of controlled substances, specifically, from **February 14, 2021 to January 24, 2023**.

Communication techniques (Instagram photographs, direct messages, and saved stories) under any Instagram accounts associated with phone number 240-722-9960 will help determine the level of communication between Franklin CARBAJAL GUERRA and unknown co-conspirators, including records that help reveal their whereabouts.

ATTACHMENT A3

Property to Be Searched

The electronic device to be searched (the "**Target Device**") is described as one light silver Apple iPhone, with silver Apple logo.



The **Target Device** is currently located at the DEA Greenbelt HIDTA Office, located in Greenbelt, MD 20770.

ATTACHMENT B3

Things to be Seized

1. All "records" (that is, documents, information, photographs, videos, communications, and any other items) contained in the **Target Device** described in Attachment A that relate to the possession with intent to distribute controlled substances and a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a) (a)(1) and (b)(1)(C) (the "**Target Offense**"), which involve Franklin CARBAJAL GUERRA, including, but not limited to, the items listed below:

a. Incoming/outgoing/missed phone call log(s);

b. SMS/MMS messages and other communications and notes;

c. Voicemail messages;

d. Photographs, audio clips, and video clips;

e. Telephone contact lists;

f. All bank records, checks, credit card bills, account information, and other financial records;

g. Records of the existence of and private messaging through social media accounts, including but not limited to, Instagram, Facebook, and Twitter; and

h. any information recording CARBAJAL GUERRA's schedule or travel.

2. Evidence of user attribution showing who used or owned the **Target Device** at the time the things described in this warrant were created, edited, or deleted, such as: logs; phonebooks; saved usernames and passwords; documents; browsing history; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user- typed web addresses.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. With respect to the search of the **Target Device**, the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

5. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

6. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably

practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT A4

Property to Be Searched

This warrant applies to information associated with Franklin CARBAJAL GUERRA, the user of calling number 240-722-9960, stored in any **iCloud Account** linked to that number that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B4

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A4 is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A4:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from **February 14, 2021 to February 8, 2024**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from **February 14, 2021 to February 8, 2024**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen (14) days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes [[fruits, contraband, evidence, and instrumentalities]] of violations of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C), those violations involving Franklin CARBAJAL GUERRA and occurring from **February 14, 2021 to February 8, 2024**, including, for each account or identifier listed on Attachment A4, information pertaining to the following matters:

(f) The stored communications and files (iMessages, photos, videos, emails, and WhatsApp) connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience the aforementioned communication techniques are used by drug traffickers to facilitate, purchase, and sale illegal drugs. On December 1, 2022, Franklin CARBAJAL GUERRA used telephone phone number 240-643-0483 attached to **Target's iCloud Account** to facilitate the purchase of illegal drugs with Yessina Morales Yaque

(g) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(h) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(i) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(j) The identity of the person(s) who communicated with the **Target's iCloud Account** as it relates to the purchase of illegal drugs. Yessina Morales Yaque

communicated with Franklin CARBAJAL GUERRA on December 1, 2022, about obtaining a controlled dangerous substance.